

日志审计中心产品功能简介

日志审计中心是 SGA 的一套日志审计系统。系统大致分为日志审计、数据报表、系统设置、日志查询和备份恢复共五大模块。

日志审计中心能够统计的内容按表排列如下：

主模块	功能模块	详细描述
日志审计	登录日志审计	基于时间段查询用户（可以为单个用户或者所有用户）的登录次数、用户的总使用时长、用户的平均使用时长。
	资源访问日志审计	基于时间段查询用户（可以为单个用户或者所有用户）对资源（可以选择为所有资源、某类型资源、某个资源）的访问次数，并且以饼状图描述各类资源。
数据报表	用户活跃程度	以用户为单位（并且显示用户姓名和用户所属组），排列出用户的登录 IP、登录的终端类型、登录次数、登录总时长、最后登录时间。并且支持下载为.csv 和.pdf 格式文件。
	资源活跃程度	基于时间段，以具体某资源为单位，排列出资源类型、访问总次数、最后访问时间。
日志查询	系统日志	基于时间段查询用户登录的客户端信息（客户端类型、）和应用使用日志，并且记录传送日志的 SGA 地址。且支持下载为.csv 和.pdf 格式文件。
	用户登录日志	记录每一次的登录或登出的记录，包括时间、用户名、登录 IP、终端类型、硬件特征码、MAC 地址、计算机名、访问时间。且支持下载为.csv 和.pdf 格式文件。
	资源访问日志	详细排列出用户（可以为单个用户或者所有用户）对资源（可以选择为所有资源、某类型资源、某个

		资源) 的访问情况。且支持下载为.csv 和.pdf 格式文件。
	文件操作日志	记录对 iBox 文件上传下载操作时的用户名、时间点、文件名(注: 目前不会记录禁止上传下载的日志)。且支持下载为.csv 和.pdf 格式文件。

说明:

1. 安装“日志审计中心”时, 请确保杀毒软件和 360 卫士/电脑管家类的保护软件都已退出;
2. 如果 SGA 在外网, 请映射日志审计中心服务器的 3306 端口。
3. 需要安装 NET Framework 4.0 才能使用

进入 SGA 后台【日志中心】→【日志服务配置】, 勾选【启用远端日志中心服务】,

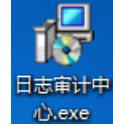
服务器地址: 日志中心服务器的地址, 即为安装了【日志审计中心.exe】的服务器。

服务器端口: 与日志审计中心服务器传送日志的端口, 必须保持与服务器上的配置一直

用户名: SGA 与日志审计中心服务器认证的用户

密码: SGA 与日志审计中心服务器认证用户的密码

The screenshot shows the 'Log Service Configuration' (日志服务配置) interface. On the left is a navigation menu with items like 'Network Configuration', 'Firewall', 'VPN', 'Application Release', 'Single Login', 'User Management', 'Authentication Management', 'Login Information', 'Certificate Center', 'Page Customization', 'System Management', 'Log Center', 'System Log', 'Log Server', and 'Log Service Configuration'. The main content area is titled '日志服务配置' and includes a radio button selection for 'Log Service' (日志服务), with '启用远端日志中心服务' (Enable Remote Log Center Service) selected. Below this are input fields for '服务器IP地址' (Server IP Address) with value '192.168.150.53', '服务器端口' (Server Port) with value '1122', '用户名' (Username) with value 'tcp', and '密码' (Password) with masked characters. At the bottom are '确定' (Confirm) and '重置' (Reset) buttons.



首先需要准备一台日志审计中心服务器，安装日志审计中心软件，安装的时候，一直下一步，在填写端口的时候，请保持与 SGA 后台的【日志中心】→【日志服务器配置】的服务器端口一致。



安装好后，后台访问端口是 7777，本机直接访问 <http://127.0.0.1:7777> 账号密码 admin/admin。

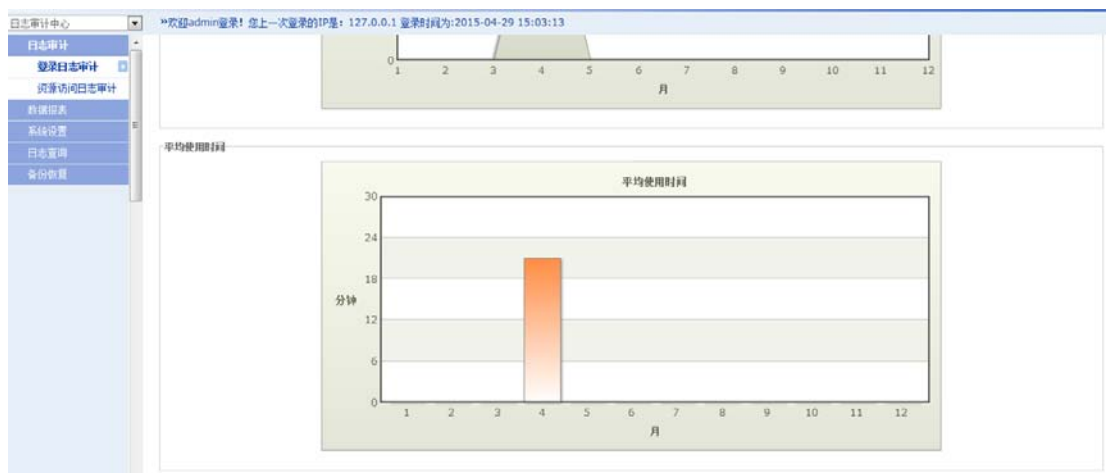
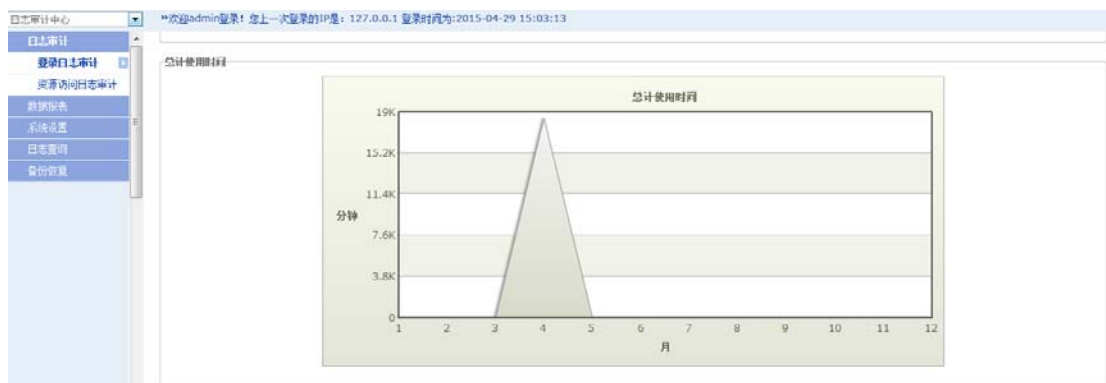
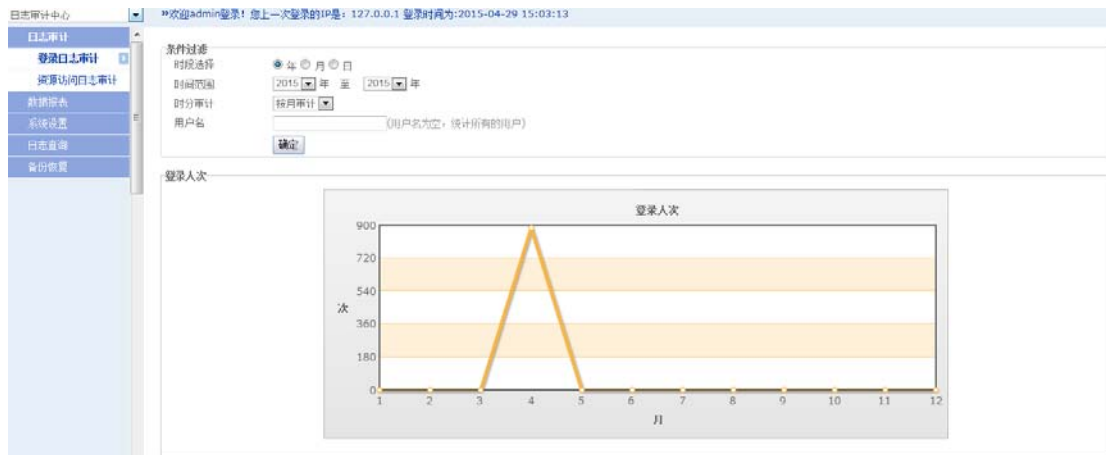
进入日志审计中心后台，【系统设置】→【发送端配置】添加用户，保证与【日志中心】→【日志服务配置】里的用户名密码一致。



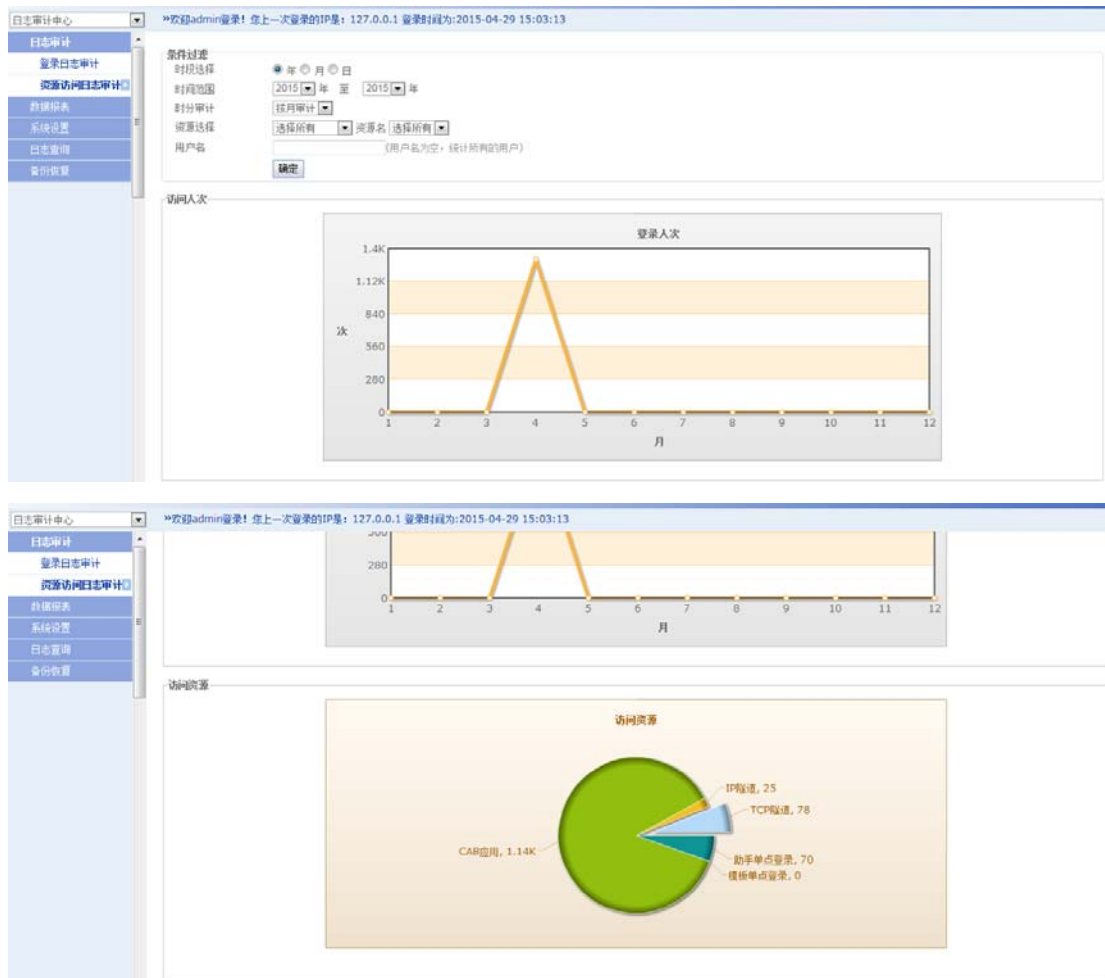
1、日志审计

【日志审计】分为【登陆日志审计】和【资源访问日志审计】两大模块。

(1)、【登陆日志审计】基于时间段查询用户（可以为单个用户或者所有用户）的登录次数、用户的总使用时长、用户的平均使用时长。



(2)、【资源访问日志审计】基于时间段查询用户（可以为单个用户或者所有用户）对资源（可以选择为所有资源、某类型资源、某个资源）的访问次数，并且以饼状图描述各类资源。



2、数据报表

【数据报表】包括【用户活跃程度】和【资源活跃程度】，主要反应了用户活跃程度和资源活跃程度。方便管理员直观了解系统登录情况。并可根据单个用户进行具体查询。

(1)、用户活跃程度

以用户为单位（并且显示用户姓名和用户所属组），排列出用户的登录 IP、登录的终端类型、登录次数、登录总时长、最后登录时间。并且支持下载为.csv 和.pdf 格式文件。

登录名	用户名	用户描述	用户IP	用户组	终端类型	登录次数	访问总时长	最后登录时间
demo			113.97.200.27	ip,tcp,demo	Windows XP	690	23时19分38秒	2015-4-27 21:41:11
demo0427			113.108.111.209	ip,tcp,demo	android_phone	5	58时4分35秒	2015-4-27 17:51:28
111			113.108.111.209		ipad	2	0时0分9秒	2015-4-27 16:43:41
dx			113.108.111.209	Terminal Server Computers,test0127_2,test0127_1,test0126_1,demo	iphone	70	17时25分52秒	2015-4-27 9:53:53
ip0424			192.168.1.124	ip	Windows 7	3	14时43分57秒	2015-4-25 9:25:29
键件			113.108.111.209	tcp,demo	iphone	4	0时11分0秒	2015-4-24 18:3:35
yingjian1			113.108.111.209		android_pad	5	0时3分28秒	2015-4-22 17:55:6
test0414			113.97.202.139	test0414	android_phone	22	4时28分19秒	2015-4-22 17:54:41
qq			113.108.111.209	ip,demo,tcp	android_phone	3	0时39分42秒	2015-4-22 15:48:54
test042101			113.118.54.206	test0421	Windows 7	18	1时21分8秒	2015-4-22 9:43:11
test0421			113.118.54.206	test0421	Windows 7	26	7时44分58秒	2015-4-22 9:34:43
qq			113.108.111.209	demo	android_pad	59	28时57分10秒	2015-4-21 17:36:38
test0412			192.168.111.99	test0412	Windows 7	5	20时8分1秒	2015-4-13 14:6:11

(2)、资源活跃程度

基于时间段，以具体某资源为单位，排列出资源类型、访问总次数、最后访问时间。

资源名称	资源类型	访问次数	最后访问时间
eylan_122	CAB应用	1	2015-4-21 17:4:39
ppp_121	CAB应用	1	2015-4-17 17:17:4
163_121	CAB应用	1	2015-4-16 16:20:42
ppp_122	CAB应用	2	2015-4-15 17:49:38
notepad_123	CAB应用	6	2015-4-15 17:12:18
163_122	CAB应用	1	2015-4-15 16:51:50
eylan_120	CAB应用	1	2015-4-15 11:25:24
书生阅读器	CAB应用	2	2015-4-15 11:25:23
vps_120	CAB应用	2	2015-4-15 11:24:11
esns1_123	CAB应用	54	2015-4-15 10:35:8
yougou	助手单点登录	1	2015-4-14 19:34:47
BS_单点	助手单点登录	2	2015-4-14 19:34:41
用友	助手单点登录	2	2015-4-14 19:33:28
华天GA_123	CAB应用	5	2015-4-14 18:28:23

3、系统设置

【系统设置】主要分为【用户管理】和【发送端配置】。

(1)、用户管理是给用户分配日志审计中心的管理账号，此账号有管理员账号和一般查看数据用户账户的权限划分。

用户名	用户权限	操作
admin	管理用户	编辑

(2)、发送端配置是建立 SGA 和日志审计中心传输日志的账号。

用户名	操作
test	编辑 删除

4、日志查询

【日志查询】里包括【系统日志】，【用户登录日志】、【资源访问日志】和【文件操作日志】。

(1)、基于时间段查询用户登录的客户端信息（客户端类型、）和应用使用日志，并且记录传送日志的 SGA 地址。且支持下载为.csv 和.pdf 格式文件。



(2)、记录每一次的登录或登出的记录，包括时间、用户名、登录 IP、终端类型、硬件特征码、MAC 地址、计算机名、访问时间。且支持下载为.csv 和.pdf 格式文件。



(3)、详细排列出用户（可以为单个用户或者所有用户）对资源（可以选择为所有资源、某类型资源、某个资源）的访问情况。且支持下载为.csv 和.pdf 格式文件。



(4)、记录对 iBox 文件上传下载操作时的用户名、时间点、文件名（注：目前不会记录禁止上传下载的日志）。且支持下载为.csv 和.pdf 格式文件。

日志审计中心 欢迎您admin登录！您上一次登录的IP是：127.0.0.1 登录时间为：2015-04-29 15:03:13

条件过滤

时间范围: 至

用户名:

每页显示:

日志下载:

操作时间	用户名	文件名	操作类型	日志来源	日志信息
2015-04-29 17:53:24	54	腾讯云新版本3.5.0.0功能.docx	下载	192.168.111.2	腾讯云新版本3.5.0.0功能.docx
2015-04-29 10:48:19	demo	99025552	删除	192.168.111.2	99025552
2015-04-29 10:48:19	demo	Chrysanthemum.jpg	上传	192.168.111.2	Chrysanthemum.jpg

5、备份恢复

可将数据保存，并且上传之前有保存的数据。

日志审计中心 欢迎您admin登录！您上一次登录的IP是：127.0.0.1 登录时间为：2015-04-29 15:03:13

数据备份与恢复

下载数据

请不要修改文件内容，否则不能上传，请勿使用下载软件下载。（ctrl+鼠标左键点击下载）

上传数据

文件路径: